The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

04/09/2013

SUBJECT:

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow For Code Execution (APSB13-12)

OVERVIEW:

Multiple vulnerabilities have been discovered in Adobe Shockwave, which could allow for code execution. Adobe Shockwave is a multimedia platform used to add animation and interactivity to web pages. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page or when a user opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Adobe Shockwave Player 12.0.0.112 and earlier versions for Windows and Macintosh

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

DESCRIPTION:

Adobe Flash Player is prone to multiple vulnerabilities that could allow for code execution. The vulnerabilities are as follows:

A buffer overflow vulnerability that could lead to code execution (CVE-2013-1383).

A memory corruption vulnerabilities that could lead to code execution (CVE-2013-1384, CVE-2013-1386).

A memory leakage vulnerability that could be exploited to reduce the effectiveness of address space randomization (CVE-2013-1385).

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

Install the updates provided by Adobe immediately after appropriate testing.
Users of Adobe Shockwave Player 12.0.0.112 and earlier versions for Windows and Macintosh should update to Adobe Shockwave Player 12.0.2.122.
Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

http://www.adobe.com/support/security/bulletins/apsb13-12.html

Security Focus:

http://www.securityfocus.com/bid/58971

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1383
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1384
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1385
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1386